

Network Management Card 4 (NMC 4) Galaxy VS Firmware 6.72.0 & Galaxy VL Firmware 12.21.0 Release Notes

New Features in Galaxy VL Firmware 12.21.0

[Top ↑](#)

For a list of features available in the NMC 4, refer to the [Network Management Card 4 Feature List](#).

Feature
Support added for Secure Syslog. Secure Syslog behaves the same way as standard Syslog, except the messages are encrypted using Transport Layer Security (TLS) before being transmitted. The NMC supports both one-way and two-way authentication between the client (the NMC) and your external Syslog server. Secure Syslog can only be used with TCP.
Reset NMC settings from Web UI and CLI. You now have an option to perform a reset of the NMC settings via the Web UI and the CLI. You can perform a <i>full reset to defaults</i> of all the NMC settings or a partial reset where the TCP/IP network settings will not be reset but all other NMC setting will be reset.
You can now upload and download files to and from the NMC using SCP.
EAPoL configuration settings are now included in the config.ini.
The file size for all files that can be uploaded is now limited to 500 KB.
The default for Bad Login Attempts is now set to 5. This had previously been set to 0.

New Features in Galaxy VS Firmware 6.72.0

[Top ↑](#)

For a list of features available in the NMC 4, refer to the [Network Management Card 4 Feature List](#).

Feature
Support added for file downloads via SCP in StruxureWare Data Center Expert and EcoStruxure IT Expert. NOTE: If devices were previously added using FTP and you want to use SCP to download files, the devices must be deleted and then re-added using SCP. For more information on adding devices, consult your StruxureWare Data Center Expert and EcoStruxure IT Expert documentation.
Support added for TLS 1.3 and support removed for the less secure TLS 1.0. NOTE: If you are using PowerChute Network Shutdown, verify that TLS 1.3 is supported in the version of PowerChute you are using. If it is not supported, you cannot register your PowerChute client.
You can now add 50 PowerChute Network Shutdown clients to the NMC Web UI (the limit was previously 12).

Feature
New SNMP Object Identifier (OID) added (<code>upsAdvStateGalaxyVseriesSpecificFault</code>) and added support for advanced state of abnormal conditions to the <code>upsAdvStateAbnormalConditions</code> OID.
Event notifications can now be configured on a per-event basis.
When an FTP session is opened and no credentials are entered, the session will timeout after 60 seconds (the timeout duration was previously 3 minutes).

Fixed Issues in Galaxy VL Firmware 12.21.0

[Top ↑](#)

Issue
It is now possible to upload new certificates and keys without deleting any existing certificates and keys. The new document will no longer get appended to any existing documents.
“Email sent successfully” is no longer erroneously reported on the Email Test page in the Web UI when the email is not sent.
For Network-Only users, the <code>user.key</code> is now listed as expected in the <code>eapol</code> directory in the CLI.
Temperature probe name is no longer incorrectly reported as “There are no sensors connected” in the Web UI instead of the configured/default probe name.
IPv6 Address changes are now visible on other interfaces including the Web UI and the UPS display.
The IPv6 network settings are now automatically applied when a configuration file is uploaded.
Email notifications will no longer be sent to the old recipient when notifications are modified for an active alarm.

Fixed Issues in Galaxy VS Firmware 6.72.0

[Top ↑](#)

Issue
When the DHCP server is unavailable, the NMC IP address no longer appears as an incorrect IP address.

Known Issues in Galaxy VL Firmware 12.21.0

[Top ↑](#)

Issue
<p>Due to security enhancements, downgrading to a previous firmware version may result in some features not working as expected. If a downgrade to a previous firmware version is required, the email authentication password will need to be reset manually.</p>
<p>Some DER format certificates cannot be uploaded to the NMC using SCP. It is recommended that PEM format certificates are used.</p>
<p>As user SSL certificates are removed, and self-signed certificates are regenerated during a reset of all NMC settings, when you are logged out after initializing a reset of all NMC settings, you must refresh the page before the browser can connect to the NMC over HTTPS using the new SSL certificates.</p>
<p>After a reset of all NMC settings, you may be presented with the error “Maximum number of sessions exceeded” when attempting to login to the NMC Web UI. The NMC should be accessible once again after 3 minutes.</p>
<p>Events related to the temperature and humidity probe connected to the Network Management Card are not displayed in PowerChute Network Shutdown if the probe is connected after registration is complete. To prevent this issue from occurring, connect the temperature and humidity probe to the Network Management Card before completing the registration in PowerChute Network Shutdown. Alternatively, connect the probe after registration is complete and restart the PCNS service.</p>
<p>When you attempt to login to the NMC Web UI following a soft reset, you will be immediately logged out following a successful login. This can be resolved by closing and restarting the web browser.</p>
<p>When using a custom email server for a configured email recipient, if a recipient authentication password is set for the email recipient, the settings for the recipient can no longer be changed using the <code>email</code> CLI command, unless the password (<code>-p</code>) and confirm password (<code>-d</code>) arguments are included. Note that the settings can be changed without any problems from the Web UI.</p>
<p>On very rare occasions following a soft reset, when SNMP is configured, the NMC does not communicate over SNMP. On these occasions, a reboot of the NMC is required to resolve the issue.</p>
<p>With some browsers, due to auto-refresh functionalities, an inactive user may not be automatically logged out if the configured session timeout is greater than 15 minutes. It is recommended that the session timeout for a user is no greater than 15 minutes. The default is set to 3 minutes.</p>
<p>SSH and HTTPS connections will be unsuccessful if the private key is not generated in PEM.</p>
<p>It is not possible to register a PowerChute client that is using IPv6 with the NMC.</p>
<p>It is not possible to generate a Technical Support debug file if you are logged into the NMC via RADIUS. You must log in as a local user to generate this file.</p>
<p>Disabling Syslog on a per-event basis does not work as expected. You can only disable Syslog using the event action per-group option in the Web UI.</p>

Known Issues in Galaxy VS Firmware 6.72.0

[Top ↑](#)

Issue
When the email recipient for notifications is modified while there is an active alarm, email notifications will continue to be sent to the old recipient for the active alarms until the alarm is cleared. Once the alarm is cleared, future email notifications will be sent to the new recipient.
The Battery Type may incorrectly be reported as “Value-regulated lead-acid, or maintenance-free” on the UPS Battery Measurements page in the Web UI when a Lithium-ion battery is used. The correct battery configuration can be confirmed in the Battery view on the UPS HMI display.
When the mode is set to “DHCP Only” in the IPv4 Settings page in the Web UI, the DHCP IP settings are incorrectly populated in the “Manual” mode section.
When the boot mode is changed from DHCP to manual in the CLI (using the <code>boot</code> command), the previously used static IP address is incorrectly assigned.
When the mode is set to “DHCP Only” in the IPv4 Settings page in the Web UI, the DHCP IP settings are incorrectly populated in the “Manual” mode section.
When the boot mode is changed from DHCP to manual in the CLI (using the <code>boot</code> command), the previously used static IP address is incorrectly assigned.

Known Issues in Galaxy VL Firmware 12.21.0 & Galaxy VS Firmware 6.72.0

[Top ↑](#)

Issue
After enabling the PowerChute Network Shutdown configuration on the NMC, while registering a PowerChute client with the NMC, you may receive the following error: “PowerChute is not receiving data from the Network Management Card.” To resolve this, perform a reboot of the NMC by pressing the Reset button on its faceplate. You will then be able to register the NMC with PowerChute successfully.
No event is logged when an SSL certificate is removed via the SSL Certificate Configuration page in the Web UI. The “New self-signed certificate loaded” event will be logged if a new certificate is manually added or auto-generated if the old certificate is deleted or out of date.
After a firmware upgrade/downgrade, the alarm count may not match between the internal and optional NMC (AP9644). To resolve this issue, press the Reset button on the AP9644’s faceplate.
You may be logged out unexpectedly from the Web UI if multiple Web UI tabs are open. This issue only occurs on Google Chrome.
After upgrading or downgrading the NMC’s firmware, a device scan request may be required to synchronize data in StruxureWare Data Center Expert.

Issue

When a user's password is changed via the `user` command in the CLI and does not meet the password requirements, a parameter error is displayed instead of "Password did not meet the requirements for a strong password."

There are discrepancies between the current time displayed in the Web UI and the CLI. The `date` command in the CLI will report the current time in real-time, whereas the Web UI will display the browser's current time with respect to the UTC value set.

NOTE: The UPS HMI will also display the current time in real-time.

The **Configure Events** screen in PowerChute Network Shutdown v4.3 displays the "Communication Established with EMC" and "Communication Lost with EMC" events. These events can be ignored as they are not supported.

When the optional NMC (AP9644) is inserted, some alarms and events are not logged on all the configured interfaces (traps, emails, Syslog, Event Log). For example, the "Lost Communication" alarm is not logged as an active alarm or sent as a trap/email.

When the Web UI is locally accessed via an internal IP address (169.254.251.1 / 169.254.252.1) and HTTP/HTTPS is disabled, you can no longer access the UI using the disabled protocol. For example, if HTTP is disabled, you cannot access the Web UI at <http://169.254.252.1>

When adding a rule via the **Firewall Configuration** page in the Web UI, the table incorrectly includes the **IP/Range/Subnet** column, which is not currently supported.

The Notification Delay and Repeat Interval features for event actions do not behave as expected. For example, you may receive multiple notifications for an active event.

You cannot connect to SNMPv1 using an IPv6 address. Use SNMPv3 as an alternative.

When the DHCP server is unavailable, the NMC IP address appears as an incorrect IP address, instead of "0.0.0.0".

When you enter a **Primary DNS Server** address in the DNS Configuration page in the Web UI, the details entered will populate the **Active Primary DNS Server** and **Active Secondary DNS Server** sections. When you enter a **Secondary DNS Server** address and switch to this network, the **Primary DNS Server** address will now be populated in the **Active Tertiary DNS Server** section.

When you log out from the NMC serial console interface, the Current Sessions page in the Web UI still shows the session as active.

The Web UI can take 25-30 seconds to load using Microsoft Edge. This is a common issue with Microsoft Edge.

File Transfer Protocol (FTP) is not available over IPv6.

When credentials are provided in StruxureWare Data Center Expert after adding the NMC via SNMP, the NMC still requires login credentials when attempting to access the Web UI.

Issue
When using IPv6 with Internet Explorer 11, you can only use the fully qualified domain name (FQDN) to access the Web UI. This is a known issue with Internet Explorer 11.
Enabling IPv6 via the CLI console port interface may cause the console connection to unexpectedly disconnect.
When Auto Configuration is disabled in the IPv6 Settings page in the Web UI, the NMC still displays the card's IPv6 address and the card is accessible using a DHCP IPv6 address.
No browser warning message is displayed in the Web UI when navigating without saving your changes.
SNMPv3 Access Control filtering is not supported. Use the Firewall to control access to SNMPv3.
When viewing the Event Details page in the Web UI for an event, you cannot disable the logging of an event to the Event Log. However, the option is still present for mass configuration of events.
When accessing the Web UI using a smartphone, the Rule Configuration table on the Firewall Configuration page is not responsive.
When an SNMPv3 profile is enabled with a valid NMS IP/Host Name, you can connect to a MIB browser of another system and not the configured SNMP profile. NOTE: The only supported value for NMS IP/Host Name for SNMPv3 is "0.0.0.0".

Copyright © 2022 Schneider Electric. All rights reserved.

<http://www.se.com>

990-6147K-001

12-2022